

Information Commissioner's Office

Consultation:

Age Appropriate Design code

Start date: 15 April 2019

End date: 31 May 2019

ico.

Information Commissioner's Office

Introduction

The Information Commissioner is seeking feedback on her draft code of practice [Age appropriate design](#) - a code of practice for online services likely to be accessed by children (the code).

The code will provide guidance on the design standards that the Commissioner will expect providers of online 'Information Society Services' (ISS), which process personal data and are likely to be accessed by children, to meet.

The code is now out for public consultation and will remain open until 31 May 2019. The Information Commissioner welcomes feedback on the specific questions set out below.

Please send us your comments by 31 May 2019.

Download this document and email to:
ageappropriatedesign@ico.org.uk

Print off this document and post to:
Age Appropriate Design code consultation
Policy Engagement Department
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

If you would like further information on the consultation please telephone 0303 123 1113 and ask to speak to the Policy Engagement Department about the Age Appropriate Design code or email ageappropriatedesign@ico.org.uk

Privacy statement

For this consultation, we will publish all responses except for those where the respondent indicates that they are an individual acting in a private capacity (e.g. a member of the public or a parent). All responses from organisations and individuals responding in a professional capacity (e.g. academics, child development experts, sole traders, child minders, education professionals) will be published. We will remove email addresses and telephone numbers from these responses but apart from this, we will publish them in full.

For more information about what we do with personal data, please see our [privacy notice](#).

Section 1: Your views

Q1. Is the 'About this code' section of the code clearly communicated?

No

If NO, then please provide your reasons for this view.

We have reviewed this draft Code through the eyes of startups and scaleups who will be tasked with the practical implementation of the concepts detailed within it.

The “about this code” section contains several substantial flaws in intent, clarity, and structure.

Who is this code for?

This area largely consists of a reference to another section, and therefore should be merged into that one and deleted from this one.

What is the purpose of this code?

This area states that “this code aims to ensure that online services use children’s data in ways that support the rights of the child to:

- freedom of expression;
- freedom of thought, conscience and religion;
- freedom of association;

- privacy;
- access information from the media (with appropriate protection from information and material injurious to their well-being);
- play and engage in recreational activities appropriate to their age; and
- protection from economic, sexual or other forms of exploitation"

While it is right and proper that these rights have a data protection element to them, what actually follows in the draft Code is the conflation of data protection concepts grounded in individual rights with matters of immediate personal safety and risk grounded in health and wellbeing. ICO thus becomes the UK's de facto child protection regulator, with the technical compliance role outsourced to startups.

We have substantial concerns that the draft Code's conflation of data protection rights with child safety, business processes with user options, and code standards with technical standards will fall onto the UK's startups to untangle on their own time and expense. We will discuss each area of concern in depth throughout this consultation response.

What is the status of this code?

We are deeply troubled by the presentation of the Age Appropriate Design Code as a piece of legislation mandated by GDPR. Under Section 123 of the Data Protection Act 2018, the production of the Code is mandated by domestic legislation, but we want to raise the critical point that the draft Code, as it is currently presented, is neither a part of GDPR nor is harmonisation with GDPR. We are concerned that the ICO is presenting the draft Code's requirements as a GDPR matter, a task mandated by GDPR, or a requirement for GDPR compliance. This draft Code, literally and legally, has absolutely nothing to do with GDPR.

The actions presented in this draft Code will create a substantial shift and amending of the Data Protection Act which will move the UK completely out of step with Europe. This will create the somewhat ironic situation where the ICO will be responsible for

leading the UK's regulatory divergence away from GDPR after Brexit.

How should we use the code?

****What the code is****

We feel that the final Code could, at some points, be presented as a useful and productive repackaging of GDPR guidance into a child-specific set of advice, instantly accessible to those startups who know that it will be an issue and want to act to tackle it. Yet the Code, at other points, amounts to a shifting of the GDPR goalposts a year after the domestic implementation became enforceable; startups and scaleups which invested the time and effort in doing the right thing, in good faith, will essentially be told to go back to square one on the presumption that they are complicit in acts of bad faith.

ICO should clarify which direction they intend to lean towards: a repackaging of existing GDPR provisions with supplementary guidance and assistance for those companies which know they will need it, or a bolt-on annex requiring fresh compliance processes from scratch for all businesses, on the presumption that a lack of participation is a lack of compliance.

****What the code is not****

Across all sections, the draft Code refers to "code standards", meaning the standards set forth in the code of practice. Many startups who will ultimately be tasked with the implementation of these requirements interpret the phrase "code standards" quite differently: they would expect to receive a series of technical guidelines and specifications, such as the WCAG standards for web accessibility. Those guidelines set forth design requirements for various forms of disability, (cognitive, blindness, motor, etc) accompanied by technical guidance and instruction, with the goal of removing obstacles to web use.

The draft code of practice document can be viewed as having a similarly extensive ambition and impact. However, it only goes halfway. It sets forth specific tiers of requirements for age bands,

but unlike the WCAG guidelines on removing obstacles, the draft Code asks for developers to create obstacles to web use. Even so, the actual drafting and the interpretation of the technical standards is left to the end implementers, despite incorrectly referring to them as “code standards”. This outsources the legal structure of compliance to developers without any technical guidance or support. This inevitably results in poor or noncompliant outcomes for end users and a lack of respect for the regulation by implementers.

If the UK truly wants to lead the way in online child protection, it should do so on a global scale through open standards, not on a national level through closed legislation. ICO should either alter the nomenclature of the plan away from “code standards” or - to be truly bold in the Digital Charter’s vision of making the internet safer - commit to collaborating with working groups and standards bodies to draft actual open technical standards, similar to the WCAG web accessibility guidelines or any number of the W3C standards, for age band requirements. The development of technical standards is a collaborative international process which takes years, not months - but it would be a more appropriate way of engaging with the challenges this issue poses than the approach outlined.

Until this oversight is remedied, the draft Code risks being a repeat of the cookie law fiasco, mandating startups to construct and deploy poorly designed, obstructive, and counterproductive barriers across the web at substantial expense - which will do nothing to serve the purpose for which they were intended.

Q2. Is the '**Services covered by this code**' section of the code clearly communicated?

No

If NO, then please provide your reasons for this view.

We found this section to be completely contradictory with the standards of age appropriate design which follow it.

The established definition of ISS services is repeated here, distinguishing between services covered, services not covered, and services “likely to be accessed”.

The latter term, “likely to be accessed”, as codified in Section 123 of the Data Protection Act 2018, is defined by this code as encompassing any and all products and services which could conceivably be accessed by an under-18 at any time. This is a bizarre and highly dangerous interpretation. It takes no account of the service’s location, purpose, target audience, size, legal status, or whether it is targeted at children at all. A more appropriate interpretation can be found in the OFT’s Principles for online and app-based games - which offers a practical standard for determining whether a service is “likely to be accessed” by children. We would strongly recommend that the ICO reconsiders this following the consultation.

As the draft Code progresses, the contradictions only deepen. The age appropriate application section states “You must apply this code so that all children are protected. If your service is likely to be accessed by children but you don’t know which users are children, you must apply the code to all users.”

The only way to determine if an ISS is being accessed by young people is through data. This mandates startups to engage in mass data collection and age gating, regardless of the actual benefit that those systems would bring for end users. Age gating is just one of the sixteen requirements mandated by this draft Code, in addition to parental controls, online tools for data rights, and five tiers of interactive privacy notices, on top of internal governance and planning procedures. Those aggregated processes are so onerous, costly, and disproportionate that they would adversely impact the ability of startups and scaleups to engage in the actual business model they went into business to do.

ICO should not use this section to soften the blow: this draft Code encompasses any product or service which exists online, and fundamentally alters the structure of the business models of the companies within its scope.

Services based outside the UK

This section confirms that non-UK businesses are more likely than not to be required to comply with the Code. Many non-UK businesses, still reeling from the compliance process for GDPR while bracing for the incoming US Federal privacy legislation, will simply refuse to undergo an even more onerous design and development process for 1/28th of the people covered by GDPR. We therefore can advise that many non-UK businesses will opt to block UK users altogether rather than be compelled to invest time and money into a nigh-impossible compliance process which, appallingly, equivocates their noncompliance with child exploitation.

Additionally, we would advise that compelling both UK and international startups to read three transcripts of CJEU case law decisions on the definition of ISS to determine whether they fall into scope, as is suggested in the “further reading” section, is not a form of practical or actionable guidance.

Standards of age-appropriate design

Please provide your views on the sections of the code covering each of the 16 draft standards

1. Best interests of the child: The best interests of the child should be a primary consideration when you design and develop online services likely to be accessed by a child.

2. Age-appropriate application: Consider the age range of your audience and the needs of children of different ages. Apply the standards in this code to all users, unless you have robust age-verification mechanisms to distinguish adults from children.

3. Transparency: The privacy information you provide to users, and other published terms, policies and community standards, must be concise, prominent and in clear language suited to the age of the child. Provide additional specific ‘bite-sized’ explanations about how you use personal data at the point that use is activated.

4. Detrimental use of data: Do not use children’s personal data in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice.

5. Policies and community standards: Uphold your own published terms, policies and community standards (including but not limited to privacy policies, age restriction, behaviour rules and content policies).

6. Default settings: Settings must be 'high privacy' by default (unless you can demonstrate a compelling reason for a different default setting, taking account of the best interests of the child).

7. Data minimisation: Collect and retain only the minimum amount of personal data necessary to provide the elements of your service in which a child is actively and knowingly engaged. Give children separate choices over which elements they wish to activate.

8. Data sharing: Do not disclose children's data unless you can demonstrate a compelling reason to do so, taking account of the best interests of the child.

9. Geolocation: Switch geolocation options off by default (unless you can demonstrate a compelling reason for geolocation, taking account of the best interests of the child), and provide an obvious sign for children when location tracking is active. Options which make a child's location visible to others must default back to off at the end of each session.

10. Parental controls: If you provide parental controls give the child age appropriate information about this. If your online service allows a parent or carer to monitor their child's online activity or track their location, provide an obvious sign to the child when they are being monitored.

11. Profiling: Switch options based on profiling off by default (unless you can demonstrate a compelling reason for profiling, taking account of the best interests of the child). Only allow profiling if you have appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or wellbeing).

12. Nudge techniques: Do not use nudge techniques to lead or encourage children to provide unnecessary personal data, weaken or turn off privacy protections, or extend use.

13. Connected toys and devices: If you provide a connected toy or device ensure you include effective tools to enable compliance with this code

14. Online tools: Provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

15. Data protection impact assessments: Undertake a DPIA specifically to assess and mitigate risks to children who are likely to access your service, taking into account differing ages, capacities and development needs. Ensure that your DPIA builds in compliance with this code.

16. Governance and accountability: Ensure you have policies and procedures in place which demonstrate how you comply with data protection obligations, including data protection training for all staff involved in the design and development of online services likely to be accessed by children. Ensure that your policies, procedures and terms of service demonstrate compliance with the provisions of this code

Q3. Have we communicated our expectations for this standard clearly?

1. Best interests of the child

No

If NO, then please provide your reasons for this view.

This section tasks British startups with the following responsibilities towards children:

keep them safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse; protect and support their health and wellbeing; protect and support their physical, psychological and emotional development; protect and support their need to develop their own views and identity; protect and support their right to freedom of association and play; recognise the role of parents in protecting and promoting the best interests of the child and support them in this task; and recognise the evolving capacity of the child to form their own view, and give due weight to that view.

While there absolutely are steps that startups and scaleups can and should take to play their roles in supporting those processes, this section tasks startups with so many fundamental obligations over the personal health and wellbeing of children - up to and including CSE - that it amounts to a demand for corporate co-parenting.

Startups embrace the role we play in keeping children safe, but we reject any demand which places primary responsibility onto companies for it.

2. Age-appropriate application

No

If NO, then please provide your reasons for this view.

This section builds a wall around the United Kingdom by mandating age gating and verification for all services, all users, and all situations:

you must apply these standards to all users unless you have robust age checks in place to distinguish children from adults. In practice, you can choose whether to apply the standards in this code to:

- all users;
- all users by default, but offer robust age-verification mechanisms to allow adults who can prove their age to opt out of some or all of those safeguards; or
- only users who are children (and not to users who are adults), if you use robust age-verification mechanisms upfront to confirm the age of each user.

The internet will not be made a safer place for children and young people by firewalling it, covering every site and service with an age verification system, and mandating companies to engage in mass surveillance, data collection, and telemetry retention which will be identifiable to every single individual user who accesses a service, even momentarily.

Demanding “robust age-verification mechanisms” of all users fundamentally alters the structure of global internet governance while outsourcing the compliance costs to British startups. This is well beyond ICO’s purview and will irreparably damage the UK’s reputation as a tech ecosystem.

3. Transparency

No

If NO, then please provide your reasons for this view.

Requiring new layers of communication on data protection topics across five broad age bands, from infancy to adulthood, mandates startups to impose very adult concepts onto the tiniest toddlers.

We are very concerned that this section conflates issues of data protection and rights with issues of personal safety and immediate risk.

4. Detrimental use of data

No

If NO, then please provide your reasons for this view.

This section asks startups to not take actions which go against “industry codes of practice, other regulatory provisions or Government advice.”

This is a monumental swathe of guidance to consider in defining detriment, some of which is backed by the rule of law and its consequences, and some of which has no actionable consequences whatsoever.

For startups working in sectors with no industry codes of practice, as is common in the tech sector, it runs the risk of asking startups to mark their own homework for the purpose of achieving compliance with the Code.

5. Policies and community standards

No

If NO, then please provide your reasons for this view.

We feel this section duplicates and reiterates the requirements already set forward in GDPR.

There is ambiguity, however, on whether policies on age restriction, behaviour rules, and content policies will be required in addition to the GDPR-mandated privacy notices. No guidance is provided on which situations will explicitly require these policies to be displayed.

6. Default settings

Yes

If NO, then please provide your reasons for this view.

We felt this section effectively duplicated the information already provided ahead of GDPR.

7. Data minimisation

No

If NO, then please provide your reasons for this view.

While we felt this section effectively duplicated the information already provided ahead of GDPR, we would, in fact, like to see it made bolder and more consistent with existing GDPR guidance, noting data retention and

data deletion as equally important; this section could, therefore, be better phrased as "Data lifecycle".

8. Data sharing

No

If NO, then please provide your reasons for this view.

While we felt this section effectively duplicated the information already provided ahead of GDPR, we thought it could have been more effectively written to reflect specific examples (such as those covered in the media) of the inappropriate sharing of children's data which this section appears drafted to address.

9. Geolocation

No

If NO, then please provide your reasons for this view.

This section of the draft Code states that "the ability to ascertain or track the physical location of a child carries with it the risk that the data could be misused to compromise the physical safety of that child. In short it can make children vulnerable to risks such as abduction, physical and mental abuse, sexual abuse and trafficking."

This is a appallingly hostile tone for a data protection regulator to take. The safe, responsible, and legal leveraging of location data carries a huge consumer benefit to both adults and young people. Used correctly, it can hugely increase the safety of users. It is helping innovation to flourish among UK startups, including Coadec's community.

We would urge the ICO to take greater care in the tone and language it uses, so that startups who responsibly leverage location data, including those offering beneficial services for children and young people, are not categorised as presumed kidnappers, abusers, rapists and sex traffickers.

10. Parental controls

No

If NO, then please provide your reasons for this view.

We found the tone of this section peculiarly legalistic, emphasising compliance with the UNCRC and Article 5(1)(a) of GDPR. As with previous sections, this legalistic approach imposes advanced data protection concepts onto under-5s who are barely cognisant of their own selves, while also, bizarrely, compelling adults to prioritise data protection frameworks over their own parental instincts.

For example, within the suggested guidelines for information across age bands, there is a preoccupation with “provid{ing} parents with information about the child’s right to privacy under the UNCRC”. We feel that, surely, advising parents to respect their children’s right to privacy as a matter of supporting their growth, development, and safety is a more reasonable approach, as opposed to mandating an explainer on parents’ role in helping the ICO to uphold international treaty obligations.

11. Profiling

Yes

If NO, then please provide your reasons for this view.

The section compels startups to take a dense and legalistic approach to one of the most critical threats to childrens’ wellbeing - algorithmic curation and profiling - they currently face.

This approach tries to achieve too much with too little clarification. For example, as with other sections, it suggests that solutions to profiling “could include contextual tagging, robust reporting procedures, and elements of human moderation” without clarifying whether these examples are in fact mandatory, or providing technical guidance for their development.

12. Nudge techniques

No

If NO, then please provide your reasons for this view.

This section of the draft Code is very clearly communicated, though somewhat randomly so. It contains clear expectations for designing for the five age bands, while other sections do not. This draws attention to the lack of clarity in other areas of the draft Code.

13. Connected toys and devices

No

If NO, then please provide your reasons for this view.

This section states “If you provide a connected toy or device, ensure you include effective tools to enable compliance with this code”.

What are those tools, who is responsible for creating them, and how will compliance be evaluated? Startups accessing a Code of Practice expect to

be given answers to questions like these within the code, not open ended questions to solve on their own time. The best answer to that question - the DCMS Code of Practice for IoT consumer security - is linked to as an external reference at the end of the section, but not discussed anywhere within it.

Related to that ambiguity, we note that this section of the draft Code discusses practical questions, such as "Provide clear information about your use of personal data at point of purchase and on set-up" and "Avoid passive collection of personal data". These are checkpoints for product and service developers to use. They are not tools for young people and their parents to use.

14. Online tools

No

If NO, then please provide your reasons for this view.

As with the section on transparency, while this section is ostensibly about helping children to exercise their data protection rights and report concerns over the misuses of their data, there is a clear conflation of immediate personal safety needs with more advanced GDPR rights such as data portability.

15. Data protection impact assessments

No

If NO, then please provide your reasons for this view.

At first glance, this section may seem to be a duplicate of guidance on DPIAs which ICO provided ahead of GDPR. However, this section suggests several new and specific questions regarding children. It must be noted that this effectively moves the goalposts for startups which have already used DPIAs, whether their services target children or not. As it stands, this section mandates fresh DPIA processes for everyone.

This will not be well received by startups, scaleups, or any business which made a good faith effort to integrate DPIA practices ahead of May 2018, nor will they appreciate ICO and government's presumption that a lack of a child-focused supplementary DPIA is an indication of bad faith.

16. Governance and accountability

No

If NO, then please provide your reasons for this view.

We feel this section was not clearly communicated. While it repeats information which was made available in the lead-up to GDPR compliance, it does not clarify what additional governance and accountability requirements will be made mandatory by this code.

Q4. Do you have any examples that you think could be used to illustrate the approach we are advocating for this standard?

1. Best interests of the child

Yes

If YES, then please provide details.

ICO has done an excellent job in devising support materials for GDPR compliance, however, GDPR was a clearly defined legal standard drafted through years of Parliamentary process and scrutiny. In contrast, the draft Code moves from an annex to GDPR to a complete shifting of its goalposts, without any of the drafting, scrutiny, or clarity provided in the years of lead-up.

For that reason, as a general principle throughout this consultation response, we feel that it will be critical for the ICO to create dedicated resources, checklists, and compliance information to support startups in implementing the Code, whether those issues are emotive and unachievable (best interests of the child) or practical and achievable (geolocation).

Any ICO guidance created to support startups in implementing the Code should reference previously produced materials as much as possible. Where the Code requires the provisions of GDPR to be renewed and refreshed, and not merely amended, those expectations must be made absolutely clear.

2. Age-appropriate application

YES/NO.

If YES, then please provide details.

3. Transparency

YES/NO.

If YES, then please provide details.

4. Detrimental use of data

YES/NO.

If YES, then please provide details.

5. Policies and community standards

YES/NO.

If YES, then please provide details.

6. Default settings:

YES/NO.

If YES, then please provide details.

7. Data minimisation

YES/NO.

If YES, then please provide details.

8. Data sharing

YES/NO.

If YES, then please provide details.

9. Geolocation

YES/NO.

If YES, then please provide details.

10. Parental controls

YES/NO.

If YES, then please provide details.

11. Profiling

YES/NO.

If YES, then please provide details.

12. Nudge techniques

YES/NO.

If YES, then please provide details.

13. Connected toys and devices

YES/NO.

If YES, then please provide details.

14. Online tools

YES/NO.

If YES, then please provide details.

15. Data protection impact assessments

YES/NO.

If YES, then please provide details.

16. Governance and accountability

YES/NO.

If YES, then please provide details.

Q5. Do you think this standard gives rise to any unwarranted or unintended consequences?

1. Best interests of the child

Yes

If YES, then please provide your reasons for this view.

The tone running throughout the draft Code presumes the guilt, bad faith, and complicity of all businesses, products, and services in the litany of threats to the best interests of the child detailed in this section. That tone places the burden of proof on startups to prove otherwise. These burdens have been mandated in response to the errors of a small but powerful handful of tech giants, not our community.

At a time when British tech startups are subject to multiple ongoing regulatory processes as well as the impact of Brexit, we question why the draft Code has been written in a way that sends the most hostile message possible to the tech sector. Mood music around the UK's openness and support of the tech sector matters in maintaining our success as a leading tech ecosystem - and we would urge a more constructive tone to be used in future engagement.

2. Age-appropriate application

Yes

If YES, then please provide your reasons for this view.

The age bands in this section, as repeated throughout the draft Code, do not create one set of requirements for startups. They create five sets of requirements for each of the sixteen different criteria, with no supporting technical standards, guidance, or comprehension of the time and financial costs inherent in them.

What the draft Code does require is an exponential increase in data collection and monitoring of all users of the UK internet, not just children and young people, although they will be the ostensible targets of that monitoring and surveillance. This will compel small companies of all shapes and sizes (who for example may run an ecommerce version of their own shop) but in particular tech startups, to engage in massive amounts of data collection, profiling, and maximisation of all users as a primary business activity in order to identify what may be, at best, passive access.

The two options put forth in this section of the draft Code - age gate all sites and everyone, or age gate all sites and everyone with opt-outs for adults and opt-ins for children - are the same options, merely phrased differently. It is clear to us that startups will be obliged to age gate their services. And consumers and companies will both suffer. This requires a radical re-evaluation.

By mandating age verification for any site or service which could conceivably be accessed by a British child or young person at some point in its lifecycle, ICO will be responsible for creating a massive state-mandated data collection system - something that is clearly not the intended remit of the proposed code.

3. Transparency

Yes

If YES, then please provide your reasons for this view.

We believe that parents would have very strong concerns about compelling preschool and young children, via startups, to be delivered information which may have a negative impact on their nascent concepts of themselves, their identities, their sense of personal safety, and their family relationships by tech companies.

The draft code, for example, suggests that developers should "provide audio or video prompts telling children to leave things as they are or get help from a parent or trusted adult if they try and change any high privacy default settings" - for children under the age of five.

Likewise, the draft Code provides a suggested mockup of a consent window which says "If you don't understand or aren't sure about this then you should leave the setting as it is, and we won't use your information in

this way.” This is a extraordinary amount of self-doubt and uncertainty to introduce into a six year old’s thought process.

The text noting that “If your online service includes a physical product, for example a connected toy or speaker you should include the icon on your packaging, highlighting online reporting tools as a product feature, and find ways to highlight reporting tools in a prominent way even if the product is not screen based” mentions nothing about the primary reporting tool in that situation: the parent or adult.

These draft requirements for transparency, in short, are a recipe for accidentally creating a culture of fear around tech and young people. This is not a role Britain’s startups should be compelled to play.

4. Detrimental use of data

Yes

If YES, then please provide your reasons for this view.

This section exists in a silo detached from the current consultation on the online harms white paper, which, in its current form, widens the scope of “detriment” from content and actions which are illegal to content and actions which are considered “harmful”. It is critical that these processes are considered together, not apart. As HMT’s Furman Review into digital markets advised, building a fragmented regulatory framework risks benefitting large incumbents and dealing a hammer blow to competition in the sector.

5. Policies and community standards

Yes

If YES, then please provide your reasons for this view.

The draft notes “If you make commitments to users about the content or other aspects of your online service then you need to have adequate systems in place to ensure that you meet those commitments. So if you say that the content of your online service is suitable for children within a certain age range then you need to have systems in place to ensure that it is.”

This conflates systems, meaning internal processes, with policies, meaning public-facing statements.

This could be abused as a means of compelling startups to disclose proprietary business information or violate non-disclosure agreements.

6. Default settings

Yes

If YES, then please provide your reasons for this view.

We are concerned that the suggestion “you should also consider whether to put any further measures in place when a child attempts to change a setting. This depends upon your assessment of the risks inherent in the processing covered by each setting and could include age verification”, leans towards the Code’s position for mandatory age gating by default, when this draft Code is in fact a consultative discussion on whether it should exist.

7. Data minimisation

Yes

If YES, then please provide your reasons for this view.

We do not feel that ICO is cognisant of the contradiction inherent in requiring startups creating sites and services not specifically aimed at children to collect data about children’s usage, and their identification as children, to determine whether that site or service is likely to be accessed by them.

In other words, in order to minimise data collection about children, startups must somehow maximise it, to the extent that data collection must become a primary business activity for everyone. This contradicts healthy data minimisation principles.

8. Data sharing

Yes

If YES, then please provide your reasons for this view.

The statement that “you should not share personal data if you can reasonably foresee that doing so will result in third parties using children’s personal data in ways that have been shown to be detrimental to their wellbeing” positions this section as a matter of general wellbeing rather than one of data protection compliance, directly contradicting the paragraphs above it.

9. Geolocation

Yes

If YES, then please provide your reasons for this view.

We noted that this section does not discuss different user needs for location data across the five age bands. As children progress through those bands, their uses of location data become less recreational and more practical: for example, the high school kid using Citymapper to get home from drama practice.

We would hope that a rigid interpretation of the Code would not infantilise that young adult under a blanket rule, or outright ban, from being able to use the app at all, under geolocation rules drawn up for toddlers playing games.

10. Parental controls

Yes

If YES, then please provide your reasons for this view.

All five age bands suggest that startups should "provide a clear and obvious sign that indicates when monitoring or tracking is active". We wonder whether consideration has been given to this requirement causing "parental monitoring blindness" - akin to cookie consent popup windows, something so ubiquitous it becomes ignored - where the child assumes they are being monitored even when they are not, and likewise, the parent grows weary of engaging in constant surveillance and merely leaves the monitoring signal on.

We also draw attention to the obvious implications of children over the age of 13 transitioning to adulthood under the watchful eye of a constantly activated parental monitoring signal, a violation of their personal privacy. The ICO must be mindful of all the rights of every user.

11. Profiling

Yes

We are very concerned about classifying every potential horror a child may encounter, from self-help images to adult content to ad targeting, as issues of profiling. Only one of those three issues, in that example, can be addressed through profiling controls.

12. Nudge techniques

Yes

If YES, then please provide your reasons for this view.

As the draft correctly notes, nudge techniques can be used positively, for example, to encourage children to protect their data, turn on their privacy settings, not disclose unnecessary information, and so forth. The proposed ePrivacy Regulation specifically encourages the use of nudge techniques to encourage users to check their privacy settings and exercise their rights.

For that reason, we are concerned that “nudge techniques” could be misinterpreted, buzzword-style, as an inherently negative feature. We would recommend more constructive phrasing suggesting positive nudge techniques which would be deemed acceptable.

13. Connected toys and devices

Yes

If YES, then please provide your reasons for this view.

Related to the previous comment, the draft section says “If you provide a connected toy or device then you need to comply with the GDPR and follow this code, and make sure that any third parties you use to deliver your overall product do so too.”

We would question why the DCMS iOT Code of Practice is not referenced here. A startup from outside the UK targeting connected devices at UK consumers, and one which could not reasonably expect to know the structure of UK government, could bring a product to market without ever knowing that the iOT Code of Practice exists as the definitive standard they are expected to follow.

14. Online tools

Yes

If YES, then please provide your reasons for this view.

We would recommend requiring the inclusion of online tools to assist children in exercising their data rights for over 13s only, as this is the mandated age for data consent established in the Data Protection Bill. Any online tools for under 13s should be aimed at parents and should be located in a parental control section.

We would advise against forcing advanced data rights concepts onto children younger than 13 without any wider context and education on issues such as human rights under the UNHCR or individual rights under the GDPR. This education process is the responsibility of multiple devolved school systems, not Britain’s startups.

15. Data protection impact assessments

Yes

If YES, then please provide your reasons for this view.

The draft Code states "You must embed a DPIA into the design of any new online service that is likely to be accessed by children."

Presuming this refers to the child-focused DPIA suggested in the draft Code, this creates the obligation for startups to engage in a "what if" compliance process even if their service is only sporadically accessed by children.

16. Governance and accountability

Yes

If YES, then please provide your reasons for this view.

The area on "what about certification schemes?" states that "Article 42 of the GDPR provides a mechanism for the establishment of certification and data protection seal schemes by which data controllers could demonstrate their compliance with the GDPR. This would be of particular benefit to children and their parents in making decisions about which online services to use (or allow their children to use) without having to assess the compliance and practice of the online service provider themselves."

This is raising an entirely separate discussion - that of a "parental seal of approval" of sorts - being created, standardised, and rolled out to companies, including startups. We are not clear whether its inclusion in the draft Code is a request for startups to begin work on that initiative, or a signal that the ICO will be taking the lead to create one.

We would also caution against publicising "parental seals of approval" which do not exist yet as a solution to parental consent. This is an area ripe for misreporting and misinterpretation.

Given this, we would suggest that the "certification schemes" area be taken out altogether.

Q6. Do you envisage any feasibility challenges to online services delivering this standard?

1. Best interests of the child

Yes

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

2. Age-appropriate application

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

The development of mandatory age gating will mean startups being reliant on the only companies which will have age verification services available for cash-tight agile startups to deploy within a three-month compliance window: adult entertainment giants. This will ironically create a system where adult service providers become the biggest winners from the code.

3. Transparency

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

4. Detrimental use of data

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

5. Policies and community standards

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

6. Default settings

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

7. Data minimisation

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

8. Data sharing

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

9. Geolocation

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

10. Parental controls

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

11. Profiling

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

12. Nudge techniques

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

13. Connected toys and devices

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

14. Online tools

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

15. Data protection impact assessments

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

16. Governance and accountability

YES/NO.

If YES, then please provide details of what you think the challenges are and how you think they could be overcome.

Q7. Do you think this standard requires a transition period of any longer than 3 months after the code come into force?

1. Best interests of the child

YES/NO.

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

Determining the best interests of the child is an open-ended commitment. It is not a regulatory compliance obligation which can, or should, be measured in a three month work package.

2. Age-appropriate application

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

Demanding “robust age-verification mechanisms” of all users fundamentally alters the structure of global internet governance while outsourcing the compliance costs to British startups. The draft Code’s demand does so without technical guidance, international governance discussions, or cognisance of the wider implications of walling off the British internet within our current political context.

This process neither can, nor should, be forced into a three month compliance window.

3. Transparency

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

Drafting accurate privacy notices for children across five age bands to new specifications, as mandated in the draft Code, will require five design and development processes, five beta testing sessions with actual children, and five feedback cycles.

For products and services specifically aimed at children, these processes can be built into the product development lifecycle. For all others,

requesting a three month compliance period can only be seen as setting them up to fail.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

4. Detrimental use of data

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

Presuming that this Code, which is specific and constrained, would take effect before the outcome of the white paper consultation is roadmapped, this section would compel startups to predict the future, to know what regulatory provisions and government advice will be issued several years from now, and to work from a definition of "detriment" which is subject to change.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

5. Policies and community standards

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

The amount of time required for startups to comply with this section will depend on what policies and community standards are deemed mandatory, as opposed to optional, and what guidance the ICO will provide on how to come into healthy compliance.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

6. Default settings

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

This section will not require a transition period of longer than three months, presuming that the existing GDPR guidance is offered as the standard to follow.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

7. Data minimisation

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

This section will not require a transition period of longer than three months, presuming that the existing GDPR guidance is offered as the standard to follow.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

8. Data sharing

No

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why

This section will not require a transition period of longer than three months, presuming that the existing GDPR guidance is offered as the standard to follow.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

9. Geolocation

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why

This is a Code point where it will be critical for the ICO to provide specific technical guidance, given that the ePrivacy Regulation revamp, which will supplement PECR and its provisions on location data, should be finalised later in 2019. This section of the draft Code, however, only discusses PECR, compelling startups to look backwards in a code which compels them to look forward.

By the nature of its inclusion in the upcoming ePrivacy Regulation, any guidance on geolocation data will take far longer than three months to be developed.

We would caution against any rules on geolocation ahead of that revamp, or aside from it, which would create regulatory divergence from the rest of Europe during and after the Brexit process.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

10. Parental controls

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why

This section of the draft code discusses parental controls as conditional, e.g. "if you provide parental controls". ICO should clarify whether parental controls will in fact be mandatory, as their age band suggestions strongly hint, and provide technical guidance for the structure and development of those controls, including how startups should "provide an obvious sign to the child when they are being monitored." This process will take substantially more than three months.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

11. Profiling

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

This section needs quite a bit of clarification and restructuring, a process which should not be outsourced to startups to solve on their own in three months.

Additionally, this section states that profiling is allowed if measures are in place to protect the child from “any harmful effects”, which ties in with the online harms white paper’s discussion on content/activities which are legal/harmful. As this Code would precede the outcome of the white paper consultation, this is an instance where the code would need to establish “harm” rather than following it, a guaranteed recipe for deviation from the actual final definition.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

12. Nudge techniques

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

The required transition period will depend on whether clear guidance is provided which defines both positive and negative nudge patterns.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

13. Connected toys and devices

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

The transition period for this section of the Code will depend on how much clarity is provided in the final version, including a distinction between user-facing tools and business-facing processes.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

14. Online tools

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

Given the lack of clarity in the draft Code's provisions on online tools, we would recommend a rewrite before giving startups three months to invent them.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

15. Data protection impact assessments

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why.

The required transition period will depend on whether ICO establishes the child-focused DPIA as a separate requirement, inclusive of templates and guidance, under the Data Protection Act 2018 (not GDPR), or whether a fresh DPIA process is mandated for all sites and services.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

16. Governance and accountability

Yes

If YES, then please provide your reasons for this view, and give an indication of what you think a reasonable transition period would be and why

As with the Policies and Community Standards section, the amount of time required for startups to comply with this section will depend on what supplemental governance and accountability procedures are deemed mandatory, which ones will be required for child-focused services and which ones will be optional for general use, and what guidance the ICO will provide on how to come into healthy compliance.

No estimate is provided about the costs which startups and scaleups can expect to incur to come into compliance with this section of the draft Code.

Q8. Do you know of any online resources that you think could be usefully linked to from this section of the code?

1. Best interests of the child

YES/NO.

If YES, then please provide details (including links).

2. Age-appropriate application

YES/NO.

If YES, then please provide details (including links).

3. Transparency

YES/NO.

If YES, then please provide details (including links).

4. Detrimental use of data

YES/NO.

If YES, then please provide details (including links).

5. Policies and community standards

YES/NO.

If YES, then please provide details (including links).

6. Default settings

YES/NO.

If YES, then please provide details (including links).

7. Data minimisation

YES/NO.

If YES, then please provide details (including links).

8. Data sharing

YES/NO.

If YES, then please provide details (including links).

9. Geolocation

YES/NO.

If YES, then please provide details (including links).

10. Parental controls

YES/NO.

If YES, then please provide details (including links).

11. Profiling

YES/NO.

If YES, then please provide details (including links).

12. Nudge techniques

Yes

If YES, then please provide details (including links).

13. Connected toys and devices

No

If YES, then please provide details (including links).

14. Online tools

YES/NO.

If YES, then please provide details (including links).

15. Data protection impact assessments

YES/NO.

If YES, then please provide details (including links).

16. Governance and accountability

YES/NO.

If YES, then please provide details (including links).

Q9. Is the 'Enforcement of this code' section clearly communicated?

No

If NO, then please provide your reasons for this view.

We felt this section lacked clarity. The area stating "We will monitor compliance with this code using the full range of measures available to us from intelligence gathering through to using our audit or assessment powers to understand an issue, through to investigation and fining where necessary" suggests that ICO will be engaging in proactive enforcement, which is to say, not in response to any specific parental or consumer complaint. The next section, "How does the ICO deal with complaints?", suggests the opposite: enforcement will be in response to specific complaints.

We would like to see clarity on whether enforcement will be proactive or reactive, and what criteria will be used to identify startups and scaleups targeted for proactive enforcement. We would also like clarification on what enforcement processes will be used where a service neither designed for, nor considered likely to be accessed by children, is nevertheless identified for enforcement action under the Code.

We would also note that this section discusses ICO's ability to enforce GDPR and PECR. As we discussed earlier, this draft Code is an extension of the Data Protection Act, not GDPR. This clarity will become more important as the UK prepares to exit the European Union.

Q10. Is the 'Glossary' section of the code clearly communicated?

Yes

If NO, then please provide your reasons for this view.

We noted a substantial inconsistency in the glossary. The glossary discusses GDPR as the European regulation and DPA 2018 as its domestic interpretation, as is amply referenced throughout the draft Code.

However, despite the draft Code placing equal emphasis on PECR, the glossary only discusses PECR as a domestic law. It omits inclusion of the ePrivacy Directive, the European directive from which PECR is derived. It also omits inclusion of the ePrivacy Regulation, the eventual

successor to the ePrivacy Directive, which is anticipated to be finalised this year.

While we appreciate that the discussion of a draft Regulation could add a layer of difficulty to the presentation of this draft Code, its omission removes half the story.

Furthermore, in our current political climate, the omission of any discussion of the current or future European parent legislation could be interpreted as a statement of the UK's intention to not comply with the ePrivacy Directive and Regulation after Brexit.

Is it?

Q11. Are there any key terms missing from the '**Glossary**' section?

Yes

If YES, then please provide your reasons for this view.

As above.

Q12. Is the '**Annex A: Age and developmental stages**' section of the code clearly communicated?

YES/NO.

If NO, then please provide your reasons for this view.

Q13. Is there any information you think needs to be changed in the '**Annex A: Age and developmental stages**' section of the code?

YES/NO.

If YES, then please provide your reasons for this view.

Q14. Do you know of any online resources that you think could be usefully linked to from **the 'Annex A: Age and developmental stages'** section of the code?

YES/NO.

If YES, then please provide details (including links).

Q15. Is the '**Annex B: Lawful basis for processing**' section of the code clearly communicated?

No

If NO, then please provide your reasons for this view.

This section is not clearly communicated. We feel that the area "When do we have to get parental consent?" should be brought out into its own main section, and enhanced with further guidance.

We also note that the "When do we have to get parental consent?" area of this section makes no reference to the section on parental controls. The obvious question for startups will be whether parental controls equal parental consent, and what actions and documentation within parental controls are considered confirmation of parental consent.

Q16. Is this '**Annex C: Data Protection Impact Assessments**' section of the code clearly communicated?

No

If NO, then please provide your reasons for this view.

The DPIA template would benefit from better design and clarity. For example, just one question in Step 2, "Describe the context of the processing", is followed by fourteen suggested prompts. We would prefer to see an approach where those questions are given their own boxes.

We would also like to see the creation of an interactive version, such as the software offered by the French CNIL, where prompts and questions are linked directly to DPA guidance.

We would caution that a redefinition of DPIAs as a documentation process in the interest of child wellbeing could inadvertently neglect other equally important areas within DPIAs across business planning, back-end development, and front-end design.

Q17. Do you think any issues raised by the code would benefit from further (post publication) work, research or innovation?

Yes

If YES, then please provide details (including links).

Finally, as data-driven startups, we were stunned by the flawed methodology used in the "Towards a better digital future: Informing the Age Appropriate Design Code" study which informed ICO's draft Code, as described on page 8 of that report:

- This research did not examine children's actual behaviour, so we are reporting on what they say rather than what they do
- Children were interviewed in groups, in which they may have tended to agree with what others were saying rather than stating their own opinion
- Children were interviewed in school and often repeated things that their teachers/parents had told them, which they knew to be the 'right' answer, but may not have necessarily done or believed

This indicates that the draft Code has been created based on guided discussions about data protection as a principle, with no active observation or qualitative data on the ways that children actually use and interact with the technology, individually and in private, which this Code stands poised to regulate.

Any further progress on this code - before publication, not after - must involve observation, data gathering, and non-directed input from the young people this Code has ostensibly been drafted to protect.

Section 2: About you

Are you:

A body representing the views or interests of children? Please specify:	<input type="checkbox"/>
A body representing the views or interests of parents? Please specify:	<input type="checkbox"/>
A child development expert? Please specify:	<input type="checkbox"/>

An Academic? Please specify:	<input type="checkbox"/>
An individual acting in another professional capacity? Please specify:	<input type="checkbox"/>
A provider of an ISS likely to be accessed by children? Please specify:	<input type="checkbox"/>
A trade association representing ISS providers? Please specify: COADEC - the Coalition for a Digital Economy http://coadec.com/contact/	<input checked="" type="checkbox"/>
An individual acting in a private capacity (e.g. someone providing their views as a member of the public or a parent)?	<input type="checkbox"/>
An ICO employee?	<input type="checkbox"/>
Other? Please specify:	<input type="checkbox"/>

Thank you for responding to this consultation.

We value your input.